



Qualys Context XDR (Extended Detection and Response) CS

Data Mapping Guide

February 13, 2023

Copyright 2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide	4
About Qualys.....	4
Qualys Support	4
Overview	5
Device Details.....	5
Supported Formats	5
Data Field Mappings	6
Qualys Internal Fields	6

About this Guide

Thank you for your interest in Extended Detection and Response (XDR). Qualys Context XDR expands the capabilities of the Qualys Cloud Platform to integrate data points from other Qualys products offer a unified view of your organization's security posture. Context XDR integrates data points (events/logs) from your enterprise's ecosystem that comprises of several heterogenous sources. This data is normalized, enriched and then categorized before storing it in the Qualys Context XDR data model. This unified database that holds data points from multiple security applications is then used to offer a 360° view of your organization's security posture — all from a single solution.

The Data Mapping Guides provide a list of the fields received through a data source and how these fields are mapped to the Context XDR data model.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit www.qualys.com.

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at <http://www.qualys.com/support/>.

Overview

Qualys Context Extended Detection and Response (XDR) can be configured to ingest data from several different data sources. Each data source has its own data points, and this Data Mapping Guide offers insight into how these data points are interpreted, normalized, and mapped in Qualys Context XDR.

This guide focuses on the data mapping between Qualys CS fields and the Qualys data model.

Note: For a complete list of sources that Qualys XDR supports, on the Qualys XDR UI, navigate to **Configuration > Data Collection > Catalog**. If the source you are looking for is not in the catalog, you can add a request for support using the **Not in the list?** card.

Device Details

- **Device Type** – Container Security
- **Device Vendor** – Qualys
- **Device Product** – Qualys CS
- **Supported Versions** – Limited Support. Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from CS using the following formats:

- **Cloud**

Data Field Mappings

This section provides a detailed mapping of the data source fields to the Qualys Context XDR.

deviceType – Container Security

deviceVendor – Qualys

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values
TRACKING_METHOD	CS_TrackingMethod	UUID
CERTIFICATE	CS_Certificate	
IP_ADDRESS	sourceIpv4	10.115.140.156
DNS_HOSTNAME	CS_DNSHostName	f5e8b9f22f01
DEVICE_TYPE	CS_Type	linux_sensor
HOSTID	deviceId	0d6f0234-7eb3-3d82-936b-f5d64034702e
OS	osDetails	Debian Linux 8.7
KERNEL_VERSION	CS_KernelVr	Linux 3.10.0-862.11.6.el7.x86_64
AGENT_VERSION	CS_AgentVr	File info for QualysAgent.exe missing from snapshot
REPORT_GENERATED_DATE	CS_ReportGenDate	2022-10-13T07:52:54.873Z
PARTIAL_REPORT_FLAG	CS_PartialRepFlag	false
SCA_SCAN_ENABLED	CS_ScaScanEnabled	false

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	Container Security
DeviceModel	CS
DeviceVendor	Qualys
DeviceHost	compXX.pXX.cisco.com
CustomerId	d656b196-edb7-45e6-8485-3748a740d002
CollectorId	ae102769-bd05-415d-af3c-2cc59681cbab
EventSourceId	1ae639f0-0944-4cbc-81ef-87c040ca9eb2
EventId	d656b196-edb7-45e6-8485-3748a740d002
CollectorReceivedTime	6/1/2021 11:29